PATENT

#19
DRUM
6-4-04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of:

Joseph Grajewski

Filed: July 19, 1999

Ser. No. 09/356,940

For: Method of Authenticating Proper Access To Secured Site and Device for Implementation Thereof

Docket No. 438 P 470

Art Unit: 2621

Examiner: B. Werner

Confirmation No. 8491

BRIEF ON APPEAL

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The present Brief on Appeal is filed in connection with the Notice of Appeal dated March 22, 2004 in the above-identified application.

REAL PARTY IN INTEREST

The real party in interest is Mandylion Labs, LLC, the assignee of all right, title and interest in the present application.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 34-54, the only claims pending, stand under final rejection and are currently appealed.

STATUS OF AMENDMENTS

An amendment containing a complete listing of pending claims and including changes to the claims was filed on February 20, 2004. The amendments to the claims were entered, but the Examiner did not find Appellant's remarks persuasive with regard to the patentability of the claims.

SUMMARY OF INVENTION.

The present invention is a portable device for generating and storing passwords and indicia representing password-secured sites, such as internet websites. Page 1, ll. 6-15. As seen generally in Fig. 1, the device is comparable in size to a keychain tag and, in fact, may be attached to a key ring in combination with a set of keys for ease of portability.

The main portion of the device 10 is a portable body member 12 that houses the remaining elements of the invention, including a microprocessor 24 for integrating all of the electronic circuits and providing a display 28 for the user. Page 2, ll. 15-19; page 5, ll. 19-28; Fig. 1. The device 10 includes non-volatile memory 40 for storing a plurality of indicia inputted by a user. Fig. 1; Page 7, ll. 1-10. Each indicia is intended to be representative of a secure site, such as an internet website, that requires a user to have a password to gain access thereto. Page 6, ll. 27-29. The device 10 further includes password circuitry 32 for generating a random password at the request of the user. Page 7, ll. 8-10. When an indicia is stored in non-volatile memory 40, a password is generated, displayed, and stored in conjunction with the indicia. Page 7, ll. 8-10. The user may then access the secure site via a host computer and configure the site

represented by the indicia to accept the randomly generated password now stored in device 10. Page 7, ll. 12-22.

A user may subsequently recall the password by accessing the device 10 and scrolling the display to find the appropriate indicia. The appropriate password is then displayed, thereby allowing the user to recall a password for a given secure site when he or she desires to gain access to the site. Page 7, ll. 4-16. The recalled password may be manually entered into the host computer or transmitted directly to the computer via an output communication port 30 of the device 10. Page 7, ll. 23-30.

The device 10 also includes a biometric sensor 26 that generates a bionic template from the presentation of a fingerprint onto an input pad 18. When the device 10 is first initialized, the template from an authorized user's fingerprint is transmitted to the microprocessor 24 and stored in memory 38, such as SRAM. Page 3, ll. 23-26; page 6, ll. 20-22. In order to access a successfully initialized device 10, the authorized user again places his or her fingerprint on the input pad 18 and a new bionic template is generated by sensor 26 and compared to the initial template stored in memory 38. Page 3, ln. 29 – page 4, ln. 1. Access to the device is only allowed if the template fingerprint matches the subsequently presented fingerprint. *Id.*

ISSUES

Whether claims 45-48 and 53 are patentable over GB 2,274,184 to McIntosh and U.S. Patent No. 5,944,824 to He. Whether claims 45-48 and 53 are patentable over GB 2,274,184 to McIntosh and U.S. Patent No. 5,732,138 to Noll. Whether claim 49 is patentable over GB 2,274,184 to McIntosh, U.S. Patent No. 5,944,824 to He, and U.S. Patent No. 6,088,143 to Bang. Whether claims 50-52 and 54 are patentable over GB 2,274,184 to McIntosh, U.S. Patent No. 5,944,824 to He, and U.S. Patent No. 6,161,185 to Guthrie et al. Whether claims 33-36, 38, 39,

40 and 41 are patentable over GB 2,274,184 to McIntosh, U.S. Patent No. 5,944,824 to He, and U.S. Patent No. 6,315,195 to Ramachandran. Whether claim 37 is patentable over GB 2,274,184 to McIntosh, U.S. Patent No. 5,944,824 to He, U.S. Patent No. 6,315,195 to Ramachandran, and U.S. Patent No. 6,088,143 to Bang. Whether claims 42-44 are patentable over GB 2,274,184 to McIntosh, U.S. Patent No. 5,944,824 to He, U.S. Patent No. 6,315,195 to Ramachandran, and U.S. Patent No. 6,161,185 to Guthrie et al. Whether claims 33-52 comply with the written description requirement.

GROUPING OF CLAIMS

The rejected claims have been grouped together in each of the rejections. Appellant contends that the independent claim in each group is representative of the remaining claims in the group and the dependent claims stand or fall with the independent base claim.

ARGUMENT

Appellant and the Examiner disagree primarily over the application of the legal standard of obviousness under 35 U.S.C. § 103(a). The Examiner rejected the claims of present application in light of two prior art combinations – either GB 2,274,184 to McIntosh ("*McIntosh*") and U.S. Patent No. 5,944,824 to He ("He"), or *McIntosh* and U.S. Patent No. 5,732,138 to Noll ("*Noll*"). As will be explained in detail with regard to each rejection, the proposed combination is legally insufficient under 35 U.S.C. § 103(a) because it does not state a *prima facie* obviousness rejection. In particular, the proposed combination does not include every element of the claimed invention, and changes the principle operation of the device of *McIntosh* to such a degree that it renders *McIntosh* unsatisfactory for its intended purpose.

I. IMPROPRIETY OF THE REJECTION OF CLAIMS 45-48 AND 53 IN LIGHT OF *MCINTOSH* AND *HE*.

Independent claim 45 calls for a device comprising: (a) a portable body member; (b) a data storage source contained in said body member; (c) user interface and communication componentry for permitting an individual to store in said data storage source a plurality of indicia each one of which is representative of a secured site; and (d) password circuitry comprising a random number generator for randomly generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia in sequence.

Both the Examiner and Appellant agree that *McIntosh* discloses a portable device having a data storage source for storing indicia that a user can then associate with a password, and that *McIntosh* also includes circuitry for generating a random sequence. In particular, *McIntosh* discloses a portable device having data storage and user interface which allows a user to store an externally generated password in memory along with indicia representing a password-protected site that is associated with the password. *McIntosh*, page 3, ln. 38-44. *McIntosh* further discloses circuitry for controlling access to the device, whereby an intended user must provide an access code to obtain access to the stored information. *McIntosh*, page 3, ln. 24-34. The device in *McIntosh* also includes a random number generator which, in response to an intended user entering an improper access code, will generate and provide a "fake" password to mislead an unauthorized user into believing that he or she successfully accessed the device. *McIntosh*, page 4, ln. 22-27.

McIntosh fails to show a device which generates a random password for an individual to use to access a protected site. The "fake" password generated in *McIntosh* does not allow the

unauthorized user to access any of the password-protected sites. *McIntosh*, page 4, ln. 41-46. Instead, the random sequence in *McIntosh* is only generated and displayed when someone improperly tries to gain access to the portable device, *i.e.*, the password generator is only used to create a fake password so that someone who improperly gains access to the device will not be able to access a protected site.

Appellant and the Examiner also agree that the secondary reference *He* teaches that random passwords are preferred over non-random passwords. *He* discloses a system for protecting the security of a computer network by standardizing the login procedures over all of the various nodes. In particular, *He* discloses a security system for enhancing the security of a computer network by using a security server that logs a user in to all network elements for which the user is authorized, thereby globalizing the user login procedure. *He*, col. 2, ll. 25-28. *He* is directed exclusively toward the security of network to node connections, and even discloses that the randomly generated network password "doesn't have to be known by the user." *He*, col. 7, ll. 65-66. The parameters for passwords, as well as the generation and storage of passwords, is controlled exclusively by the system password initialization module regardless of whether the password in chosen randomly or manually. *He*, col. 8, ll. 4-12. *He* is thus directed toward protecting ***inter-network*** security from electronic eavesdropping, and does not address security of the ***user-to-network*** connection. *He*, col. 7, ll. 42-47. By contrast, *McIntosh* is directed to solely to improving the security of the ***user-to-network*** connection by protecting the accessibility of passwords stored in a user's personal device. More importantly, *He* does not teach allowing users to choose their own passwords, and definitely does not discuss how a user should handle personal password storage and retrieval.

A. The Proposed Combination Does Not Disclose Each and Every Element of the Claimed Invention

According to the Examiner, the general teaching in *He* that random passwords are preferred over non-random passwords is sufficient to motivate the structural modification of *McIntosh* to include a random password generating circuit to generate passwords for the user to gain access to the secure sites represented by the stored indicia, and therefore renders the claimed invention obvious under 35 U.S.C. § 103(a). The changes to *McIntosh* proposed by the Examiner go far beyond the simple teaching in *He* that randomness of passwords is preferred for network security purposes. The Examiner proposes a structural modification to the user device in *McIntosh* to generate passwords, rather than merely to store server generated passwords – the only function contemplated by *McIntosh*.

While *He* teaches that randomized passwords are beneficial for improving network security, the reference does not motivate or suggest generating randomized passwords ***at the user side*** or, more appropriately, ***at a user password storage device***. This positioning of randomization at the user side is expressly recited in all of the rejected the claims, which call for the portable device to include circuitry for generating random passwords that are subsequently associated with indicia representing protected sites.

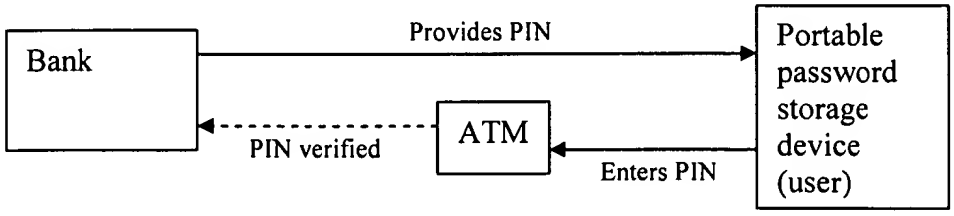
He only discloses that it is preferable for a computer network to randomly generate network use only passwords. In fact, *He* states that a user need not know the network security password. The purported motivation from *He* has been taken out-of-context, and is insufficient to motivate the structural redesign of *McIntosh* to accomplish an entirely different goal because *He* is limited to enhancing network security and does not apply to user security. *See Bausch &*

Lomb, Inc. v. Barnes-Hind/Hydrocurve, 796 F.2d 443 (Fed. Cir. 1986) (failure to consider reference in its entirety was improper when considering obviousness).

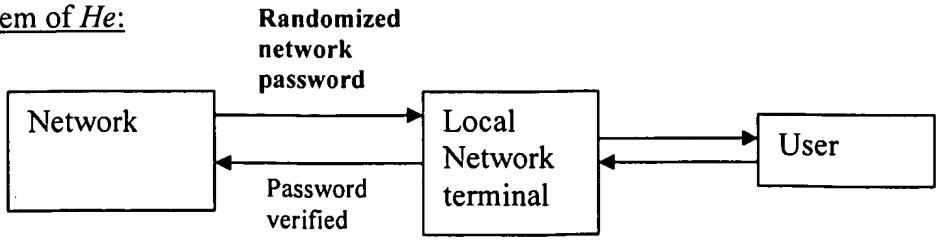
The actual result one would reach by following the teaching in *He* demonstrates that the combination proposed by the Examiner does not disclose each and every element of the claimed invention as required by 35 U.S.C. § 103(a). In a system including the device of *McIntosh*, *He* at best teaches that a network or server should generate random passwords. In the Examiner's proposed combination, *He* would only motivate a bank server, such as that disclosed in *McIntosh*, to generate a randomized password and then send it to the account holder for storage in the device of *McIntosh*. *He* lacks the necessary motivation, however, to alter the user's personal storage device to form the claimed invention, as *He* only teaches improving network security with randomized passwords generated exclusively at the ***server*** side, rather than the ***user*** side.

Following is a schematic representation of *McIntosh* and *He* illustrating how a proper combination of the teachings in each reference still would not form the claimed invention:

System of *McIntosh*:

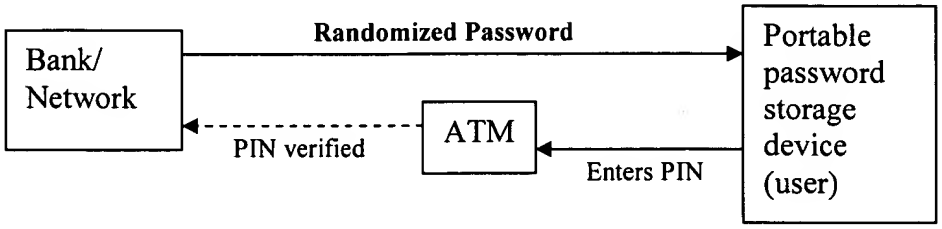


System of *He*:



The Examiner contends that this teaching of a randomized intra-network password is sufficient to motivate the proposed changes to the user storage device of *McIntosh*. As the following diagram illustrates, a change according to *He* would not achieve the structure of claimed invention, as *He* only motivates randomizing by a server or network, not a user.

Properly Modified *McIntosh* according to *He*:



When *McIntosh* is modified according to *He*, randomizing occurs at the bank (*i.e.*, the server or network), rather than at the personal storage device. As *He* deals exclusively with the use of a randomized password to protect intra-network security, *He* at best only motivates a change in *McIntosh* at the bank side of the schematic. Thus, the application of the motivation of *He* to *McIntosh* does not result in a portable device including a random password generator, as proposed by the Examiner. Instead, the randomization must occur at the network level, as this is the location where *He* teaches randomness is preferred. The combination proposed by the Examiner thus does not result in a device that meets each and every limitation in claim 45 as required for a *prima facie* case of obviousness under 35 U.S.C. § 103(a).

The creation of the password at the user side is an express limitation in claim 45, which recites that the claimed portable device includes "password circuitry for generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia." This express element in the claims clearly places the point of generation of the passwords at the portable device, rather than at the secure site to which the user

of the device wishes to gain access. Neither *McIntosh* nor *He* motivate the generation of passwords at the user-side as recited in the claims, because the motivation in *He* relied on by the Examiner does not teach the desirability of making the ***specific combination*** set forth in claim 45. *In re Kotzab*, 217 F.3d 1365, 1369-70 (Fed. Cir. 2000). The Examiner's rejection is therefore the product of impermissible hindsight analysis as the changes proposed to the device in *McIntosh* are not motivated by *He*.

As explained by the court in *In re Kotzab*, 217 F.3d 1365, 1369-70 (Fed. Cir. 2000):

> Most if not all inventions arise from a combination of old elements. Thus, every element of a claimed invention may often be found in the prior art. However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. Rather, to establish obviousness based on a combination of the elements disclosed in the prior art, there must be some motivation, suggestion or teaching of the ***desirability of making the specific combination*** that was made by the applicant. (internal citations omitted) (emphasis added)

The court in *Kotzab* subsequently overturned the Patent Office finding that the claimed invention covering a single sensor controlling multiple valves was obvious in light of the prior art disclosing multiple sensors controlling multiple valves. In particular, the court stated that:

> In this case, the Examiner and the Board fell into the hindsight trap. The idea of a single sensor controlling multiple valves, as opposed to multiple sensors controlling multiple valves, is a technologically simple concept. With this simple concept in mind, the Patent and Trademark Office found prior art statements that in the abstract appeared to suggest the claimed limitation. But, there was no finding as to ***the specific understanding or principle within the knowledge of a skilled artisan that would have motivated one with no knowledge of Kotzab's invention to make the combination in the manner claimed.***

Id. at 1371 (emphasis added). Here, as the court in *Kotzab* said is often likely to occur, the Examiner found references that individually disclose many of the elements claimed by

the Appellant. The Examiner did not, however, properly identify how one of ordinary skill would be ***motivated to make the claimed combination***, because the Examiner did not identify a specific motivation to randomize passwords at the user side for contemporaneous storage with indicia identifying the secure sites. Instead, the motivation identified by the Examiner (*i.e.*, "random is better") is insufficient to support the Examiner's proposed structural modifications because *He* does not motivate the claimed combination of having a portable device perform the randomizing and storage of passwords.

B. The Proposed Modification to *McIntosh* Changes the Principle Operation of the Device and Renders it Useless for its Intended Purpose

Even if the general teaching in *He* that randomness is better is sufficient to motivate the specific combination of elements recited in claim 45, the alterations to the device disclosed in *McIntosh* that are proposed by the Examiner would impermissibly change the principle operation of the device and render it unsatisfactory for its original purpose, in contravention of the requirement for a valid obviousness rejection. *See* MPEP § 2143. The mere fact that *McIntosh* ***could*** be modified as proposed does not mean that the prior art actually suggests the modification. *See In re Fritch*, 972 F.2d 1260 (Fed. Cir. 1992).

McIntosh is concerned with storing the passwords associated with a protected site that are externally generated by the protected site and then provided to a user. If the device in *McIntosh* were altered as suggested by the Examiner, however, it would create havoc with the ability of a user to access the systems disclosed in either *McIntosh* and *He*.

If the device in *McIntosh* were changed to generate its own passwords, a user would no longer be able to access any of the password-protected sites, because the sites contemplated by *McIntosh* and *He* control the identity of passwords, not the user. In *He*, for example, the network

administrator is responsible for setting the parameters of the passwords. *He*, col. 7, ll. 56-63. If a user generated his or her own password, this security feature would be lost. Moreover, a user of the device in *McIntosh* that was modified to generate a password would not be able to access a site where the identity of the password was controlled entirely on the server side, as in the system disclosed in *McIntosh*. While a user could certainly generate his or her own password, that password is ineffective because the server is entirely unaware of the new user-generated password. The modified device proposed by the Examiner would therefore not work in the very system addressed by *McIntosh*.

It is fundamental that a proposed modification should not render the prior art device unacceptable for its intended purpose or change its principal mode of operation. *See* MPEP § 2143.01 (citing *In re Gordon*, 733 F.2d 900, 221 U.S.P.Q. 1125 (Fed. Cir. 1984) and *In re Ratti*, 270 F.2d 810, 123 U.S.P.Q. 349 (C.C.P.A. 1959)). The Examiner's proposed combination does just that, as it changes the device in *McIntosh* in such a way that it will not work for its expressly intended purpose. Thus, even if the modification proposed by the Examiner is motivated by the general teaching in the prior art, the proposed combination would violate the standards required for a proper 35 U.S.C. § 103(a) combination and claim rejection.

II. IMPROPRIETY OF THE REJECTION OF CLAIMS 45-48 AND 53 IN LIGHT OF *MCINTOSH* AND *NOLL*.

Noll, like *He* discussed above, simply describes an apparatus for creating random passwords and generally discloses that random passwords are better than non-random passwords. *Noll*, col. 1., ll. 45-52. While *Noll* teaches the general use of randomized passwords over non-randomized passwords to improve security, it fails to provide the necessary motivation to modify the structure of the portable device of *McIntosh* to include circuitry for generating random

numbers for association with the indicia of secure sites, as presently claimed. As described with regard to *He* above, a general suggestion that a random password is better than a non-random password is legally insufficient to render the claimed invention obvious under *Kotzab* and the standard required by 35 U.S.C. § 103(a), because it fails to motivate each and every element the claimed combination and results in a combination that is unfit for its principal purpose.

III. IMPROPRIETY OF THE REJECTION OF CLAIM 49 IN LIGHT OF *MCINTOSH*, *HE*, AND *BANG*.

In addition to the basic elements of the portable device, claim 49 further calls for "an output communications port connected to output circuitry for directly transmitting said password to said selected indicia to said secured site." According to the Examiner, *Bang* discloses a device including a communication port for directly transmitting password and motivates the modification of *McIntosh* to simplify input procedure and avoid disclosure of passwords to third parties. As discussed above, the proposed combination of *McIntosh* and *He* is improper and does not meet the requirements for a valid obviousness rejection under 35 U.S.C. § 103. Accordingly, claim 49 is believed to be patentable over the cited references regardless of whether *Bang* motivates the addition of a communication port in the claimed invention.

IV. IMPROPRIETY OF THE REJECTION OF CLAIMS 50-52 AND 54 IN LIGHT OF *MCINTOSH*, *HE*, AND *GUTHRIE*.

In addition to the basic elements of the portable device, claim 50 calls for means for prompting a user to change a password after a predetermined time. According to the Examiner, Guthrie discloses structure corresponding to such means and motivates its inclusion in the claimed device. As discussed above, the proposed combination of *McIntosh* and *He* is improper and does not meet the requirements for a valid obviousness rejection under 35 U.S.C. § 103.

Accordingly, claim 50 is believed to be patentable over the cited references regardless of the disclosure in *Guthrie* relative to circuitry for prompting password changes.

V. IMPROPRIETY OF THE REJECTION OF CLAIMS 33-36, 38, 39, 40 AND 41 IN LIGHT OF *MCINTOSH*, *HE*, AND *RAMACHANDRAN*.

In addition to the password generating and associating capabilities of the basic device, claim 33 calls for:

> a biometric interface unit engaged with said body member;
>
> a non-volatile memory mounted to said body member;
>
> biometric circuitry for generating and storing in said non-volatile memory an initialized biometric template upon presentment of the person's unique biometric parameter to said biometric interface unit, and generating a second biometric template upon subsequent presentment of the person's unique biometric parameter to said biometric interface unit;
>
> compare circuitry for enabling said device only if said second biometric template is substantially identical to said initialized biometric template.

According to the Examiner, *Ramachandran* discloses the claimed biometric authorization elements and motivates their combination in present invention. As discussed above, the proposed combination of *McIntosh* and *He* is improper and does not meet the requirements for a valid obviousness rejection under 35 U.S.C. § 103. Accordingly, claim 33 is believed to be patentable over the cited references regardless of the disclosure in *Ramachandran* relative to biometric circuitry.

VI. IMPROPRIETY OF THE REJECTION OF CLAIM 37 UNDER 35 U.S.C. § 103(A) IN LIGHT OF *MCINTOSH*, *HE*, *RAMACHANDRAN*, AND *BANG*.

Claim 37 adds the element of an output communications port, as discussed with regard to the rejection of claim 49 in light of *McIntosh*, *He*, and *Bang*. As discussed above, the proposed

combination of *McIntosh* and *He* is improper and does not meet the requirements for a valid obviousness rejection under 35 U.S.C. § 103. Accordingly, claim 37 is believed to be patentable over the cited references regardless of the disclosure in *Bang* relative to communication ports.

VII. IMPROPRIETY OF THE REJECTION OF CLAIMS 42-44 IN LIGHT OF *MCINTOSH, HE, RAMACHANDRAN,* AND *GUTHRIE.*

Claim 42 calls for means for prompting a user to change the password, as discussed with regard to the rejection of claims 50-52 and 54 in light of *McIntosh*, *He*, and *Guthrie*. As discussed above, the proposed combination of *McIntosh* and *He* is improper and does not meet the requirements for a valid obviousness rejection under 35 U.S.C. § 103. Accordingly, claim 42 is believed to be patentable over the cited references regardless of the disclosure in *Guthrie* relative to circuitry for prompting password changes.

VIII. IMPROPRIETY OF REJECTION OF CLAIMS 33-52 FOR FAILING TO COMPLY WITH THE WRITTEN DESCRIPTION REQUIREMENT.

Claim 33 calls for "password circuitry for generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia in sequence." The Examiner determined that this element could be interpreted to mean generating all of the passwords at the same time, associating all of the passwords with indicia at the same time, and then storing all at once. As the specification only discloses generating a single password, associating that password with an indicia, and then storing, the Examiner determined that the claim failed to comply with the written description requirement.

In rejecting a claim under section 112, first paragraph, an examiner must set forth express findings of fact which: (1) identify the claim limitation at issue; and (2) establish a *prima facie* case by providing reasons why a person skilled in the art at the time the application was filed

would not have recognized that the inventor was in possession of the invention as claimed in view of the disclosure of the application as filed. MPEP § 2163.04.

Here, the Examiner alleges that the claims are improper because they cover associating numerous passwords with numerous indicia all at once, when the disclosure only teaches sequential storage. Rather than identify a specific claim ***term*** or ***limitation*** not described in detail in the specification, the Examiner creates an "indefinite" limitation in an apparatus claim by construing the claim to recite a way of ***using*** the claimed invention not disclosed *in hac verba* in the specification. This analysis is improper in two regards.

First, section 112, paragraph 1 does not require an inventor to describe every possible way in which a claimed invention may be used. Such a requirement is untenable. For example, the inventor of a new pocketknife need not describe every way in which a user could whittle a block of wood to support claims directed toward the structure of the knife.

Second, the Examiner's interpretation of the limitation at issue is erroneous given the plain language of the claim and the patent disclosure. The language in the claim clearly recites "***each*** of said plurality of passwords is uniquely associated with a respective ***one*** of said plurality of indicia." The only reasonable interpretation of this language is that the claimed invention associates each password with one indicia, and not all of the passwords with all of the indicia all at once. This interpretation of the claim language is fully supported by the description of the invention in the specification. Nevertheless, Appellant has added the limitation "in sequence" to the rejected claims to further clarify the operation of the claimed invention and obviate the written description rejection.

CONCLUSION

In conclusion, the rejection of the claims under 35 U.S.C. § 103(a) is improper as the modification proposed by the Examiner does not disclose each and every limitation of the claimed invention. Additionally, the proposed modification changes the principle operation of the primary reference and renders it useless for its intended purpose. Finally, the rejection of the claims under 35 U.S.C. § 112, ¶ 1 has not been properly applied, and has been overcome by Appellant through a post-final amendment entered by the Examiner. Reversal of the rejections in this Appeal is respectfully requested.

Respectfully submitted,

Dated: May 24, 2004

By: _____
George R. McGuire
Reg. No. 36,603

BOND, SCHOENECK & KING, PLLC
One Lincoln Center
Syracuse, New York 13202-8530
(315)218-8515

APPENDIX

33. A device for use by an authorized individual having a unique biometric parameter to obtain information for use in accessing a secured site, the device comprising:

a. a portable body member;

b. a biometric interface unit engaged with said body member;

c. a non-volatile memory mounted to said body member;

d. biometric circuitry for generating and storing in said non-volatile memory an initialized biometric template upon presentment of the person's unique biometric parameter to said biometric interface unit, and generating a second biometric template upon subsequent presentment of the person's unique biometric parameter to said biometric interface unit;

e. compare circuitry for enabling said device only if said second biometric template is substantially identical to said initialized biometric template;

f. a data storage source;

g. user interface and communication componentry for permitting said individual to store in said data storage source a plurality of indicia each one of which is representative of a secured site; and

h. password circuitry for generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia in sequence.

34. The device according to claim 33, further comprising indicia selection circuitry for permitting said individual to use said user interface and communications componentry to select one of said plurality of indicia when said device is enabled.

35. The device according to claim 34, further comprising recall circuitry for recalling from said data storage source the one of said passwords that corresponds with said selected one of said plurality of indicia.

36. The device according to claim 35, further comprising output circuitry and a display mounted to said body member for visually displaying said password associated with said selected indicia.

37. The device according to claim 36, further comprising an output communications port connected to said output circuitry for directly transmitting said password corresponding to said selected indicia to said secured site.

38. The device according to claim 33, wherein said password circuitry comprises a random number generator.

39. The device according to claim 33, wherein said biometric interface unit is a fingerprint reader.

40. The device according to claim 33, wherein said user interface and communications componentry comprises means for communicating a preselected string of predetermined length of characters in said data storage source.

41. The device according to claim 40, wherein said means for communicating a preselected string of predetermined length of characters in said data storage source comprises a plurality of arrow keys mounted to said portable body member which may be manipulated and actuated by said individual and which electronically communicate with said device upon actuation by said individual.

42. The device according to claim 33, further comprising means for prompting said individual to change a password corresponding to a predetermined indicia after expiration of a predetermined period of time.

43. The device according to claim 42, wherein said means for prompting said individual to change a password after expiration of a predetermined period of time comprises a clock and circuitry coupled thereto which actuates said device to display a predetermined message.

44. The device according to claim 43, wherein said password circuitry will generate a new password and associate said new password with the corresponding one of said indicia for which said prompt was actuated.

45. A device for use by an authorized individual to obtain information for use in accessing a secured site, the device comprising:

a. a portable body member;

b. a data storage source contained in said body member;

c. user interface and communication componentry for permitting said individual to store in said data storage source a plurality of indicia each one of which is representative of a secured site; and

d. password circuitry comprising a random number generator for randomly generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia in sequence.

46. The device according to claim 45, further comprising indicia selection circuitry for permitting said individual to use said user interface and communications componentry to select one of said plurality of indicia when said device is enabled.

47. The device according to claim 46, further comprising recall circuitry for recalling from said data storage source the one of said passwords that corresponds with said selected one of said plurality of indicia.

48. The device according to claim 47, further comprising output circuitry and a display mounted to said body member for visually displaying said password associated with said selected indicia.

49. The device according to claim 48, further comprising an output communications port connected to said output circuitry for directly transmitting said password corresponding to said selected indicia to said secured site.

50. The device according to claim 45, further comprising means for prompting said individual to change a password corresponding to a predetermined indicia after expiration of a predetermined period of time.

51. The device according to claim 50, wherein said means for prompting said individual to change a password after expiration of a predetermined period of time comprises a clock and circuitry coupled thereto which actuates said device to display a predetermined message.

52. The device according to claim 51, wherein said password circuitry will generate a new password and associate said new password with the corresponding one of said indicia for which said prompt was actuated.

53. A method for creating, storing, and managing a password, comprising the steps of:

a. providing a device comprising a portable body member, a data storage source contained in said body member, user interface and communication componentry for permitting said individual to store in said data storage source a plurality of indicia each one of which is representative of a secured site, and password circuitry comprising a random number enerator for randomly generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia;

b. entering preselected indicia representative of a secured site into said device in response to a prompt generated by said device;

c. instructing said device to randomly generate a string of characters of predetermined length that is representative of a password in response to a prompt generated by said device, wherein said password is uniquely associated with said indicia entered in step b; and

d. repeating steps b and c in sequence for as many times as desired and permitted by said data storage source.

54. The method of claim 53, further comprising the step of instructing said device to generate a replacement password for said password created in step c in response to a prompt displayed on said portable body member after a predetermined period of time since said password was created in step c.

AF/2621

PTO/SB/21 (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/356,940
Filing Date	07/19/1999
First Named Inventor	Joseph Grajewski
Art Unit	2621
Examiner Name	B. Werner
Attorney Docket Number	438P470

Total Number of Pages in This Submission

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance communication to Group
- ☒ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) (please Identify below):

  postcard

Remarks

The Commissioner is hereby authorized to charge the Deposit Account or credit any over-payment to Deposit Account 50-1546 for said fees

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	George R. McGuire Bond Schoeneck & King, PLLC
Signature	
Date	05/24/04

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	George R. McGuire		
Signature		Date	05/24/2004